Security Measurement as a Trust in Cloud Computing Service Selection and Monitoring

Osman Ghazali
School of Computing, Universiti Utara Malaysia, Sintok 06010, Malaysia
Email: osman@uum.edu.my

Abubakar Magira Tom, Hatim Mohd Tahir, Suhaidi Hassan, Shahrudin Awang Nor, Ahmad Hanis Mohd Shabli
School of Computing, Universiti Utara Malaysia, Sintok 06010, Malaysia
Email: {magiratom, hatim, suhaidi, shah, ahmadhanis}@uum.edu.my

***Abstract*—With the increase in the number of cloud service offerings by the cloud service providers nowadays, selecting the appropriate service provider becomes difficult for customers. This is true since most of the cloud service providers offer almost similar services at different costs. Thus, making cloud service selection a tedious process for customers. The selection of the cloud services from the security standpoint needs a distinct consideration from both the academia and the industry. Security is an important factor in cloud computing. Thus, any exploited vulnerability will have a negative effect on cloud computing adoption by customers. Hence, little attention has been paid to cloud service monitoring and selection from a security perspective. To solve this issue, we propose a security measurement as a trust (SMaaT) in the cloud computing selection. Finally, we propose Analytical Hierarchical Process (AHP) for service selection from the customers' perspective.**

***Index Terms* – Service Selection, Security Measurement, Cloud Service Provider, Quality of Service, Service Level Agreement.**

I. Introduction

The cloud computing customers get remarkable processing power, data storage, availability, and scalability of cloud services and resources at minimum cost. These resources are accessible via the cloud computing paradigm which is increasingly adopted by the organizations and companies. The services include; elasticity, multi-tenancy, high service utilization and service subscription. The National Institute of Standards and Technology (NIST) describes the cloud computing as a prototype that consents abundant, suitable, on-demand network access to a mutual pool of configurable computing services like the network, servers, data storage and software applications that can be rapidly delivered and released easily. The cloud computing aims to provide small and medium enterprises with the capability to adopt cloud services to maximize their cost and return on investment (ROI). The cloud computing comprises of three layers; the Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). The SaaS supports organizations evade capital expenditure as well as pay for only the functionalities they need, such as maintenance, etc. Although, SaaS is not immune to security risks and vulnerability. The risks may include difficulty to switch from cloud service providers, risks of lock-in, privacy concern, access control and security, quality assurance, data ownership as well as the lack of standardization [1]. The PaaS offers access to application programming interface, programming languages and the development of middleware that enables cloud users to design custom applications, without installation or configuration of the cloud development environment [2]. The cloud-based platform can be categorized into full or partial PaaS. The Full PaaS gives the client the ability to develop solution entirely via the web application user interface without the need of installing a thin client (web browser). The Partial providers convey some tools to the client as a service yet requires users to install applications to develop solutions on their own devices [3]. One of the challenges of using PaaS is compatibility [2]. Nonetheless, Security also remains a big concern in the public cloud arena. Thus, public cloud limits the ability of customers to secure and control their data in a geographical location effectively. The IaaS provides users with the ability to create, deploy as well as maintaining virtual machines and storage. Thus, security, policies, governance and the physical location of the data in the cloud arena is still a concern in IaaS adoption. The Cloud users have to deal with updates and patches of their applications unlike SaaS and PaaS platform, and it may expose all parties of the risks of security and privacy incidents [2]. The extremely vigorous, dispersed and less translucent nature of cloud services makes trust and selection of appropriate cloud service provider (CSP) very tricky. Again, with the surge in the provision of cloud services, it is getting difficult for cloud customers to decide which CSPs can achieve their promised quality of service (QoS) as agreed upon in the Service level agreement (SLA). For example, some cloud service providers offer almost similar services at different costs [4]. Hence, given the distributive nature of cloud computing, discovering the right CSP is difficult for

Manuscript received December 28, 2016, revised May 14, 2017.

doi: 10.12720/jait.8.2.100-106

consumers considering privacy, security and legal requirements involved in the cloud [5]. Therefore, some cloud consumers may be concerned with performance and availability, while other users may be highly concerned about privacy and security of their data in the cloud. Thus, making it difficult for consumers to evaluate cloud QoS and SLAs objectively. Buyya et al. point out certain QoS parameters that are crucial for cloud customers like the service request time, cost, reliability, and trust or security [3]. Thus, QoS should not be stagnant and needs to be updated dynamically (periodically) over time due to the continuous changes in the network as well as the changing business environment. So, customers should have special consideration in a cloud setting since they are practically the consumers of the cloud services and resources. Additionally, it is insufficient just to subscribe to cloud computing without considering the functional and non-functional requirement implications. Trust is among the key factors that hinders cloud adoption and blind trust is not perfect and ought to be supported by effective justification [6]. Hence, many organizations and companies are starting to recognize and realize the benefits of cloud computing, but, as with emerging technology and new approaches, there is the anxiety of ambiguity and concern about the maturity of technology [7]. Likewise, performance concerns can deter some companies and organizations from adopting cloud computing for transaction and data rigorous applications. Since, some providers run short of capacity, either by over provisioning of many VMs or saturating the internet link and customers in a far geographical location may experience latency [7]. In a survey conducted by IDC, 75% of cloud customers rate security and privacy concern as the most factors that hinders cloud computing adoption [7].

The Cloud Monitoring refers to the process of observing and tracking applications and resources in the cloud arena. Thus, the cloud monitoring is very crucial for the CSPs and the customers as it involves dynamically tracking the quality of services parameter [8]. Conversely, the cloud monitoring is used in several situations such as; the performance, SLA management, security, billing and troubleshooting. Similarly, the CSPs must ensure the SLAs are not violated and as well as ensure high resource utilization to avert exorbitant maintenance of resources. Hence, monitoring, tracking and reporting SLA violations is a very tedious process and time consuming for cloud customers and CSPs. This necessitates the need for a continuous monitoring of cloud resources and it's SLAs like the availability, privacy and security, etc. by both CSPs and customers. In this paper, we aim to come up with a security monitoring and measurement in cloud computing from the customer's perspective. The customers will be able to select certain CSPs based on their security specifications. Security must be balanced between securities, usability and simplicity. Security is the responsibility of everybody, both the cloud customers and CSPs.

The rest of the paper is organized as follows; in Section II, we present Service Level Agreement (SLA) and Quality of Service (QoS) in cloud computing. Section III presents related work. Section IV presents service quality monitoring, security quality of service, security quantification and analytical hierarchical process. Section V presents the contribution and Section VI presents conclusion and future work.

II. Service Level Agreement

Service Level Agreement (SLA) refers as an explicit declaration of expectations and obligations as well as mutual understanding that exists between two or more organizations (i.e. the CSPs and the service users). The SLAs are the main elements of the governance of the cloud computing infrastructure. The SLAs describes the threshold and the financial penalties associated with violations of these thresholds like the availability, performance and security respectively [9]. Hence, a well-designed and documented SLA will significantly improve understanding and limit conflicts as well as enable the resolution of SLA violations [9]. The SLA basics comprise of Service Level Objectives (SLO), Key Performance Indicator (KPI). The SLOs are the objectives that will be achieved while the KPI are a set of measurable KPIs with thresholds to verify if the stated objectives are achieved or not. The SLAs reflects the rules that drive the service relationship between the cloud providers and the organization [10]. The cloud computing SLAs are termed as the Cloud Service Agreement (CSA). The CSAs are agreements written with a clear mindset and expectations for services between cloud customers and the Cloud Service Providers (CSPs), but also should focus on the cloud carrier, cloud broker and the cloud auditor [9]. Thus, SLAs are based on the cloud service delivery models such as the Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Generally, the CSA comprises of three key artifacts, namely, the customer agreement, acceptable use policy and the SLA [9]. However, well-established cloud service providers tend to be inflexible with their CSAs whereas, less established CSPs seem to be flexible to a certain extent but, they tend to exaggerate their services to attract more clients [9]. In [11], the researcher provides a complete description of the SLA components and break the SLA into nine phases, namely purpose, restrictions, validity period, scope, parties, service level objectives (SLO), penalties, optional services and administration. In [12] classified SLA lifecycle into three phases namely the creation phase, the operation phase, and the removal phase. Nevertheless, Sun Microsystems internet data center group (2002) provides a more detailed and comprehensive SLA. The SLAs life cycle is broken down into six phases; they are; discover service, define SLA, Establish Agreement, Monitor SLA violations, Terminate SLA and Enforce Penalties for the SLA violations [13]. It is essential for cloud customers to know the service providers upfront. In the definition of SLA, once the CSP is discovered, customers should

identify their quality of service (QoS) as well as their Service Level Objectives (SLO). The performance, availability, and security should be well understood by customers. The agreement establishment allows the template design and includes all the aspects of the SLA components [13]. The Monitoring of SLA violations plays an important role in determining whether LSO is violated or not. The termination of SLA is quite challenging considering the cloud data may be dispersed in a different location and different data center (for backup). The service provider should ensure that all data of customers are completely deleted. Finally, the enforcement of SLA violation penalties should be clearly defined by the cloud service provider. If customers observe any deviation from the promised performance and security, then the customer should file and report the violation in a timely manner.

A. Quality of Service in Cloud Computing

The cloud computing is used by numerous organizations and companies to host and access thousands of services and resources at any given time and in any geographical location. Thus, cloud consumers may be dispersed in diverse locations and each consumer may require different quality of service (QoS) specifications [14]. The QoS is believed to be one of the main issues that are yet to be resolved. Hence, QoS is the fulfillment of the Service Level Agreement (SLA). The SLA outlines the agreed service quality that the service provider must provide to the cloud consumers. Normally, consumers may expect a certain level of QoS to be met by the cloud service providers (CSPs). But, forecasting or even assuring QoS in the distributive cloud arena may be challenging [15]. The Cloud customers face challenges in selecting appropriate CSP's that suits their requirement specifications due to the increase of the CSPs [16]. This is because quite some service providers offer almost similar services at different costs. This necessitates the need for quality of service and cloud service providers who will meet functional and non-functional requirements specifications of customers. Many CSPs tend to exaggerate (provide fake ratings) to make their business more appealing and prosperous, so as to attract gullible customers [17]. Hence, there is a need for service quality monitoring from the customers' perspective. Several Research has developed frameworks, mechanisms, and systems to ensure QoS in SLA are met by the CSP's. The quality of service model comprises of five phases, namely reliability, responsiveness, assurance, empathy and tangible. Reliability gives the ability to access cloud service reliably and correctly. For example, like sending packets promptly. The Responsiveness is the readiness of cloud service providers to help cloud customers get their promised quality of service (QoS) as written in the SLA. The Assurance involves conveying trust and confidence in the cloud service providers. Thus, Security/Privacy is an important QoS specification, the security and privacy will improve trust and confidence in cloud services. The Empathy allows cloud service providers to be considerate and meet customers QoS needs. The Tangible in cloud computing involves the attention given to organizations by cloud service providers in term of helping them when in need. The following is a brief description of some of the proposed frameworks, techniques, and systems in this regard.

III. Related Work

In [18] states that it is the responsibility of the cloud users to ensure that suitable security measures are put in place, depending on the security level agreed upon in the SLA agreement. This is extremely challenging since most users do not even know what security requirement they need talk less of monitoring the security in the distributed cloud arena. The Cloud customers need guarantees regarding the security of their virtual machines, operating within the IaaS infrastructure [19]. Thus, the VM security seems complicated for customers since customers do not know where exactly their VMs is executing as well as the requirements of customers and their expectations of what is measured in the cloud arena. Hence, security, trust and privacy issues are an open research area that requires more attention from both academia and industry [13]. Hence, many cloud service providers tend to exaggerate (provide fake ratings) to make their business more appealing and prosperous, so as to attract more customers [17]. Thus, making cloud service, selection very difficult. Both technical as well as usability issues limit the adoption of the security level agreement (SecLAs) [20]. The Cloud Service Providers (CSPs) are trying to make customers trust their services. However, the cloud users should also be able to measure as well as confirm if the said security will satisfy their security requirement specification [20]. In [19] argues that; monitoring the VMs security health is a big issue because cloud users have limited privileges that prevent them from collecting good security measurements to monitor the health of the VMs. Additionally, there is an absence of a technique for the cloud customers to measure the cloud security level as publicized by the CSPs are delivered as agreed in the SLAs. Hence, many authors propose different techniques, algorithms and ranking parameters or metrics improve the cloud service selection process. In [20] proposed an AHP-Based Quantitative approach for assessing and comparing cloud computing security. The authors introduced a method for performing a qualitative analysis of the security level by the CSPs. The Analytical Hierarchical process (AHP) is used for comparing and benchmarking of the cloud security as provided by the CSPs as written in the SLA. The cloud customers will be able to select security based on their security requirements specifications. The proposed framework is validated using cloud SecLAs found in the Cloud Security Alliance (CSA) public STAR repository. However, it will be difficult to publish the security of cloud service providers since the cloud computing performance and security is dynamic and fuzzy in nature. Hence, the security may change at any time and will also incur high computational overhead when comparing hundreds of CSPs concurrently. Luna et al [21] presented a security metrics framework for CSPs security assessment. The authors further proposed

Reference Evaluation Methodology (REM). Hence, no further elaboration was made on how to develop and evaluate the proposed framework. In Zhang et al [19] proposes a CloudMonatt architecture to detect and monitor security health like the vulnerability of the Virtual Machine (VM) and provide a secure protocol to request and receive security. The authors implemented the property-based attestation using the openStrack application in the cloud. The performance evaluation solves two issues; the overhead of the VM is launching because of new security requirement specifications and also the overhead of attestation during runtime. But, the focus is only on the attack. Mazur et al [18] propose a Mitigating cloud computing security risks using a self-monitoring defensive scheme and offer a solution that leverages intelligent multi-agent systems and network ontology, to provide automated defense from known and un-known malware security risks. The authors further examine the underlying security risks associated with the cloud computing and compare possible ways to mitigate the security risks as well as solutions. But, the proposed self-system was not implemented and it may cause computational overhead. Again, how the security risks are measured is missing. In Bernsmed et al [20] presented a method for managing the Security Level Agreement (SecLAs) life cycle in the settings of federated cloud computing services. But, no further elaboration of techniques was presented. In Luna et al [22] proposed a QUANTS as a service as a security benchmark methodology that rests on the notion of Quantitative Policy Trees (QPT) to quantitatively and qualitatively compare cloud security level agreement. The authors further proposed Reference evaluation methodology (REM) that allows different cloud service providers to compose security, but only in lower level nodes. This is the major shortcomings of the proposed QUANTS model.

IV. Cloud Monitoring

A cloud monitoring refers to the process of observing and tracking applications and resources. The cloud monitoring is very crucial for CSPs and customers as it involves dynamically tracking the quality of services parameter [8]. However, the cloud monitoring is used in "various context" such as the performance, service level agreement management, security, billing, and troubleshooting. Thus, CSPs must ensure that SLAs are not violated and as well as have to certify high resource utilization to avert overpriced maintenance of the cloud resources. Hence, monitoring, tracking and reporting SLA violations is a very tedious process and time consuming for cloud customers. This necessitates the need for a continuous monitoring of cloud resources and its SLAs like the availability, privacy etc. by both CSPs and cloud customer's. In this paper, we aim to develop security monitoring, measurement in cloud computing from the customer's perspective. Thus, customers will know the security of the CSPs before subscribing to the cloud. This is especially true for security involves ensuring that system and data are free of all malicious manipulations. But security must be balanced between security, usability and simplicity. The cloud monitoring and SLAs are correlated because one SLA has an impact on the other [19]. Furthermore, security monitoring is very crucial in a cloud computing architecture [4], [8]. The security monitoring is lacking behind other features like performance monitoring [8]. The deficiency of security SLAs and the lack of a standardized method for comparing security objectively makes it almost impossible for CSPs to offer trustworthy services when third-party providers are involved [23]. Thus, the security SLAs will escalate the trust in CSP, but will also enable the comparison between CSPs objectively based on their security features.

A. Service Quality Monitoring

With the increase in the offerings of cloud computing services, it is ever more challenging for consumers to decide which cloud service providers (CSP's) can fulfil their promised quality of service (QoS) as specified in the Service level agreement (SLA) [4]. For example, quite some service providers offer almost similar services at different costs [4]. Hence, most of the cloud customers are not clear about the quality attributes that they require to satisfy their requirements. Again, most at times, providers make certain claims and guarantee about certain threshold level of quality in the SLA. Thus, failure is imminent due to the unpredictable nature of the internet infrastructure. The highly transparent, distributive as well as non-transparent nature of the cloud makes trust management challenging. Again, due to the growth and expansion of cloud computing services, the QoS parameters and measuring units gets diverse at times and contradict [24]. Thus, the available QoS models mostly focus on cost-benefit analysis or performance evaluation. Thus, QoS model should be holistic in nature to cover most of the quality aspect. Hence, it is challenging for cloud clients to differentiate between good and bad cloud service providers. The cloud CSP's need to be trustworthy enough to ensure that their SLAs are met and no deviation from the promised SLA is recorded as well as SLA verifications. However, QoS should be defined via a range of multiple parameters to satisfy consumer's service requirement specifications [24], [25].

B. Security Quality of Service

Suitable security and privacy solutions must be adopted before cloud computing potentials will be fully realized [6]. Saripalli and Walters [26] also argue that, security is a main issue, because, confidentiality, integrity, authenticity and auditability is crucial for businesses, legal and competitiveness of organizations. Hence, many organizations are reluctant to adopting cloud computing due to security concerns. This is true since organizations would practically hand over their data to the CSPs with little or no control. Again, lack of methods and techniques for cloud users to access as well as ensure advertised security levels are actually delivered by the CSPs [20]. The CSPs are trying hard to influence cloud users to have confidence in their security, which in

the real sense is not feasible. Similarly, with the growing number of CSPs in the market today, it is difficult to compare quantitatively the security offered by the CSPs to meet users' security requirements [20]. The security life cycle stages comprise of publishing, negotiation, commitment, provisioning, monitoring and termination [23].

Numerous techniques were adopted by various CSPs to achieve security in cloud computing and vary in nature. Hence, analyzing and quantifying CSPs services based on security is a very challenging task. Customers should know the security level of the CSPs providers. Furthermore, Security Assurance in cloud computing has recently been looked at by the cloud community such as; "European network and information security agency (ENISA)" [4] and the Cloud Security Alliance (CSA). The ENISA and CSA have come up with a good security level agreement to access security offered by the CSPs. The STAR encompasses cloud security level agreement as Consensus Assessments Initiative Questionnaire (CAIQ). The CAIQ comprises of 171 security questions (with answers like Yes or No) [27]. Thus, the CAIQ security questions are further broken down into Compliance, Data Governance, Facility Security, Human Resource Security, Information Security, Legal, Operations Management, Risk Management, Release Management, Resilience and Security Architecture. However, there is a gap on methods and techniques to quantitatively quantify security assurance in the cloud computing arena [27]. Additionally, one of the challenges of developing a security benchmark usually depends on the unknown rather than what is known [28]. Below are some of the research about security quality monitoring.

Pavlidis et al, [6] present a trustworthy service selection framework by incorporating Computer Aided Software Engineering (CASE) tool for new activity in cloud service selection. Weight is assigned to each privacy and security satisfiability. The satisfiability value is between 0 and 1 respectively. The allocation of security and privacy weights is conducted by security and privacy experts. This is the major shortcoming of the model, because, biases may exist. In [26] presents a qualitative impact and risk assessment framework for cloud security (QUIRC). The framework assesses security risks involved in cloud computing. The QUIRC framework compares and access security quantitatively and allows cloud customers aware of the security of CSPs. However, the final risk assessment is based on expert opinion. This is a measure short coming of the QUIRC framework. This is because biases may exist in the risk assessments. Luna, Langenberg and Suri [27] proposes a benchmarking qualitative and quantitative security in the cloud. Thus, the quantification is based on Quality Policy Trees (QPT) data structure. The authors provide a security benchmark and qualitative or quantitative approaches for users to evaluate security. However, the proposed benchmark does not show how security is broken down, what techniques are used to calculate and assign trust weight. Again, the security attributes are general and not specific. Security parameters and metrics are not shown. Neto and Vieira [28] propose trustworthiness benchmarking in cloud computing trust as a measure to benchmarking security. Even though trustworthiness benchmark cannot provide same security guarantees, it is still crucial and can easily fulfil most of the security benchmark requirements [28]. Shaikh and Sasikumar [29] proposes a trust model for measuring the security strength of cloud computing. The proposed trust model will measure the security attributes and strength by computing a trust score. However, in the real cloud environment, user comments and feedback cannot be used to evaluate trust. This is because, the cloud CSPs do not provide their security details and most at times, customers are not even aware of what security they require.

TABLE I. TABULAR SUMMARY OF SECURITY QUALITY OF SERVICE

Authors	Parameters/Framework	Comments
[6]	Trustworthy Service Providers Selection Framework	A Trustworthy CSPs selection framework based on security and privacy requirements. This is a good model towards security service selection. But, the allocation of security and privacy weights is conducted by security and privacy experts. Also, there is also no algorithm or simulation of the proposed model.
[20]	AHP based Quantitative approach	An AHP based Quantitative approach for accessing and comparing cloud security. Analytical hierarchy process allows comparison and benchmarking of security. But, no algorithm and simulation provided
[26]	QUIRC framework	The framework assesses the security risks associated with cloud computing. But, the final risk assessment is based on expert opinion and expert may be bias
[27]	QUANTSaaS Benchmarking for Quantitative and Qualitative measurements	QUANTSaaS Allows users to quantitatively and qualitatively measure security. But, the QUANTSaaS does not show how security is weighted are assigned. Again, the security is too general and not specific to certain security parameters that the layman can understand.
[28]	Trustworthiness Benchmark	The trust framework may not provide the same kind of security guarantee that users require. Again, the framework is still new and seems to be useful. But, more work is needed to show how it works and how the trust score is generated quantitatively
[29]	Trust model for measuring security strength	The trust values are just assigned. No algorithm was proposed to show how the trust values are assigned. Dynamic and stagnant trust values cannot be used to assess the security strength of the cloud computing.

C. Security Quantification

In this stage, cloud user will select cloud service providers based on customers' security requirements. Thus, the CSPs will be ranked using data published by the service providers. The security quantification process will comprise of disaster recovery plan (DRP), incident response plan (IRN), business continuity plan (BCP) certifications, policies and etc. The defined service level objectives (SLO) are the distinctive elements of the cloud Security Level Agreement (SecLAs). Our work complements the work [20]. We further adapt Analytical Hierarchical Process (AHP) to rank the security aspect and trust values will be adequately assigned to the security parameters respectively. The AHP allows calculation of attribute weights depending on user preference and the estimation of interdependencies between the attributes. The AHP process includes the following steps; the problem decomposition, priority judgment and priority aggregation. The first phase constructs a hierarchy structure that models the relationship between the goals and the CSPs process. The QoS attributes as well as the service candidates and the pairwise comparison is then conducted in the second phase, to decide the comparative importance of the criteria and local ranking of the service candidates. Finally, the general ranking of the services based on the cloud security attributes are generated.

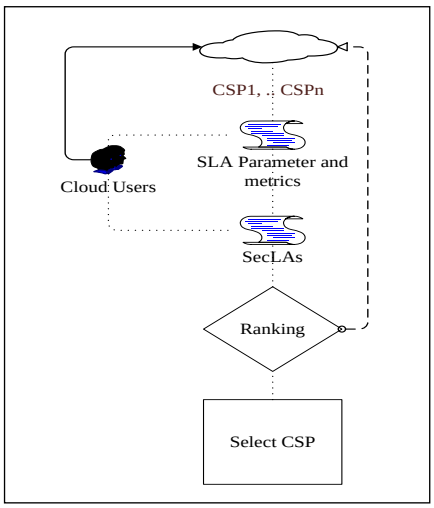

Figure 1. SMaaT framework

The proposed Security Measurement as a Trust framework enables cloud customers to specify their security requirements in upfront before selecting cloud service providers. The SMaaT provides users with a lists of security attributes and metrics for them to select, after selecting the security, the system will compare (rank) the cloud service providers and select the ones that best suits customer's security requirement specifications.

D. Analytical Hierarchical Process

The analytical process comprises of four phases, namely; the structure, weight assignment, pairwise comparison and attribute aggregation to get a final trust score of cloud services. The hierarchical structure allows the organization of Security Level Agreements (SecLAs) hierarchy and defines the structure from top down approach (Highest to lowest). Thus, the data used is adapted from the CIAQ [30]. "The CIAQ comprises of the Compliance (CO), Data Governance (DG) Information Security (IS)" and others. In this paper, only CO, DG and IS will be used to evaluate our proposed SMaaT framework. The weight assignment allows the cloud customer to select their Security Service Level Objectives (SSLO). The weight will be "1" for "Important", "05" for "Less Important" and "0" for "None" required respective ly. The pairwise comparison is a way of modeling values to a quantitative meaningful metric detonating the required security attributes. The CSPs offer almost similar services, but will different costs [4]. Hence, comparison matrix will be used to compare the diverse cloud service providers in the cloud. We complement the work of [20] but, we look at security measurement from a different angle. Our proposed security measurement will be looked at using published (assumed) security attributes such as the disaster recovery plan, incident response plan, security certification etc. and the history of any security incident

V. Contribution

This paper aims to solve the problem of cloud security monitoring and service selection from the cloud customer's perspective. We propose a SMaaT framework that will allow cloud customers to select cloud service providers (CSPs) based on their security requirement specifications. Finally, we propose Analytical Hierarchical Process (AHP) model to solve the problem of comparison and multi-criteria decision problem for cloud customers.

VI. Conclusion and Future Work

Different CSPs offer almost similar services, but at different costs. It is challenging to compare different CSPs security quantitatively. Since, measuring security deals with measuring uncertainty, which in a real sense is difficult to achieve. Hence, cloud computing security monitoring is still in an infant stage. More research is needed on ways to quantify security from the customer's perspective. We look at security measurement from a different angle and not the usual key length or encryption size calculation. We propose security measurement using published (assume) security attributes such as the disaster recovery plan, incident response plan, security certification etc. and the history of any security incident. We also propose the use of Analytical hierarchical process (AHP) to solve the problem of multi-criteria decision making (MCDM) for customers. The SMaaT framework allows users to select cloud services based on their preferred security requirement specifications. However, we are going to measure security based on STAR repository. We will further explain how we measure security in the SMaaT model from the customer's perspective. We intend to build this

application and evaluate it with other proposed model in future. We intend to design a prototype to evaluate the proposed SMaaT model by evaluating a real cloud data set. Many people perceive security differently. Thus, a standardized cloud security monitoring, measurement criteria remain a gap.

REFERENCES

[1] M. Janssen and A. Joha, "Challenges for adopting cloud-based software as a service (saas) in the public sector.," *ECIS*, 2011.

[2] J. Gibson, R. Rondeau, D. Eveleigh, and Q. Tan, "Benefits and challenges of three cloud computing service models," in *Proc. 2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN)*, 2012, pp. 198–205.

[3] R. Buyya, C. S. Yeo, and S. Venugopal, "Market-oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities," in *Proc. 2008 10th IEEE International Conference on High Performance Computing and* Communications, 2008, pp. 5–13.

[4] S. K. Garg, S. Versteeg, and R. Buyya, "SMICloud: A framework for comparing and ranking cloud services," in *Proc. 2011 Fourth IEEE International Conference on Utility and Cloud Computing*, 2011, pp. 210–218.

[5] T. M. Abubakar and G. Osman, "Cloud service selection: A critical review," *Am. Sci. Publ.*, vol. In Press, 2017.

[6] M. Pavlidis, H. Mouratidis, C. Kalloniatis, S. Islam, and S. Gritzalis, "Trustworthy selection of cloud providers based on security and privacy requirements: Justifying trust assumptions," Springer Berlin Heidelberg, 2013, pp. 185–198.

[7] N. Leavitt, "Is cloud computing really ready for prime time," *Growth*, 2009.

[8] D. Petcu, "SLA-based cloud security monitoring: Challenges, barriers, models and methods," Springer International Publishing, 2014, pp. 359–370.

[9] A. T. Velte, T. J. Velte, and R. C. Elsenpeter, *Cloud Computing:A Practical Approach*. McGraw-Hill Professional, 2010.

[10] O. Rebollo, D. Mellado, E. Fernández-Medina, and H. Mouratidis, "Empirical evaluation of a cloud computing information security governance framework," *Inf. Softw. Technol.*, vol. 58, pp. 44–57, 2015.

[11] L. Jin, V. Machiraju, and A. Sahai, "Analysis on service level agreement of web services," *HP June*, 2002.

[12] S. Ron and P. Aliko. "Service Level Agreements," (2001). [Online]. Available: http://ing.ctit.utwente.nl/WU2/.

[13] W. Linlin and R. Buyya, "Grid and cloud computing: Concepts, methodologies, tools and applications" - *Google Books*, Illustrate. IGI Global, 2012.

[14] S. K. Garg, S. Versteeg, and R. Buyya, "SMICloud: A framework for comparing and ranking cloud services," in *Proc. 2011 Fourth IEEE International Conference on Utility and Cloud Computing*, 2011, pp. 210–218.

[15] J. M. Pedersen, M. T. Riaz, J. C. Junior, B. Dubalski, D. Ledzinski, and A. Patel, "Assessing measurements of QoS for global cloud computing services," in *Proc. 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing*, 2011, pp. 682–689.

[16] S. M. Habib, S. Ries, and M. Muhlhauser, "Towards a trust management system for cloud computing," in *Proc. 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*, 2011, pp. 933–939.

[17] S. K. Chong, J. Abawajy, M. Ahmad, and I. R. A. Hamid, "Enhancing trust management in cloud environment," *Procedia - Soc. Behav. Sci.*, vol. 129, pp. 314–321, 2014.

[18] S. Mazur, E. Blasch, Y. Chen, and V. Skormin, "Mitigating cloud computing security risks using a self-monitoring defensive scheme," in *Proc. the 2011 IEEE National Aerospace and Electronics Conference (NAECON)*, 2011, pp. 39–45.

[19] T. Zhang and R. B. Lee, "CloudMonatt," in *Proc. the 42nd Annual International Symposium on Computer Architecture - ISCA '15*, 2015, pp. 362–374.

[20] A. Taha, R. Trapero, J. Luna, and N. Suri, "AHP-Based Quantitative Approach for Assessing and Comparing Cloud Security," in *Proc. 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*, 2014, pp. 284–291.

[21] J. Luna, H. Ghani, and D. Germanu, "A security metrics framework for the Cloud - IEEE Xplore Document," in *Proc. Security and Cryptography (SECRYPT)*, 2011, pp. 245–250.

[22] J. Luna, H. Ghani, and T. Vateva, "Quantitative assessment of cloud security level agreements: A case study," *Proc. Secur. Cryptogr.*, pp. 64–73, 2012.

[23] K. Bernsmed, M. G. Jaatun, P. H. Meland, and A. Undheim, "Security SLAs for Federated Cloud Services," in *Proc. 2011 Sixth* International *Conference on Availability, Reliability and Security*, 2011, pp. 202–209.

[24] M. Salama *et al.*, "A novel QoS-Based framework for cloud computing service provider selection," *Int. J. Cloud Appl. Comput.*, vol. 4, no. 2, pp. 48–72, 2014.

[25] J. Sidhu and S. Singh, "Improved TOPSIS method based trust evaluation framework for determining trustworthiness of cloud service providers," *J. Grid Comput.*, pp. 1–25, Feb. 2016.

[26] P. Saripalli and B. Walters, "QUIRC: A quantitative impact and risk assessment framework for cloud security," in *Proc. 2010 IEEE 3rd International Conference on Cloud Computing*, 2010, pp. 280–288.

[27] J. Luna Garcia, R. Langenberg, and N. Suri, "Benchmarking cloud security level agreements using quantitative policy trees," in *Proc. the 2012 ACM Workshop on Cloud computing security workshop - CCSW '12*, 2012, p. 103.

[28] A. A. Neto and M. Vieira, "TO BEnchmark or NOT TO BEnchmark security: That is the question," in *Proc. 2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSN-W)*, 2011, pp. 182–187.

[29] R. Shaikh and M. Sasikumar, "Trust model for measuring security strength of cloud computing service," *Procedia Comput. Sci.*, vol. 45, pp. 380–389, 2015.

[30] CSA. Consensus Assessments : Cloud Security Alliance. (2016). [Online]. Available: https://cloudsecurityalliance.org/group/consensus-assessments/. [Accessed: 03-Dec-2016].

Osman Ghazali is an Associate Professor and Deputy Dean of the School of Computing, Universiti Utara Malaysia. Osman holds a Ph.D. degree in Information Technology (Networking) from Awang Had Salleh Graduate School, Universiti Utara Malaysia (AHSGS). He did his post-doctoral as a research scientist at the School of Engineering & Applied Science, Aston University (EAS) in 2012. In 2011, Osman was the Head of Computer Science Department, School of Computing, Universiti Utara Malaysia. Before that, from 2009 to 2011, he was the Technical Chairperson at the University Teaching and Learning Center, Universiti Utara Malaysia. Dr. Osman has more than 100 publications as refereed book chapters and refereed technical papers in journals and conferences. He is a senior member of the InterNetworks Research Laboratory. He is also a member of the IEEE and the ACM.